Email
Email is a communication tool; there are many email service companies such as Gmail, Microsoft Outlook, Yahoo!, and many others.

Investigators and the IRB should determine whether the email service is suitable for use in research in reference to regulations such as HIPAA and other data privacy laws. While employers provide email for employees, investigators should determine if the office email is an appropriate tool for communication with research participants. For example, email encryption may be essential to protect a research participant’s protected health information. If a non-employee email service, such as a third-party email service is used, keep in mind that each email service company has its own terms of use agreement and privacy policies. Users must follow rules dictated by the terms of use, some of which are common sense while others are based on the company’s specific policies.

Investigators and the IRB should take into account that communicating with a research participant via email could lead to possible problems in interpretation of both questions and responses. The research participant will be unable to read visual and auditory cues, such as facial expressions and voice intonation, which are often used to convey and/or emphasize meaning. Thus, investigators may need to ask explicit clarifying questions to accurately interpret responses and provide additional information to ensure potential participants understand the questions and information being communicated.

Below are model statements investigators may adapt to describe email.1

Sample: Email
There is no guarantee your email information will remain confidential. Your confidentiality can be protected by the protections in place on the technology being used and additional precautions suggested by the research team. While efforts are made to protect your data, confidentiality of your data cannot be guaranteed.

The technology you use to write and send your email(s) can increase the protection of your information. For example, you can use a strong password, anti-virus and anti-malware protections, and a secure wireless network.

The research team will work with you on how to increase your security when using email. They will explain steps you can take including how to encrypt your emails, what information you should avoid including in your emails, and warnings to watch for (e.g. emails from unknown users, or emails asking for more information than the research team explained you would be asked to share). If you receive a suspicious email, contact the research team immediately.

When sending emails, make sure to limit the personal information you include, such as your full name, address, social security number, and other personal information. An email account can be hacked by an unauthorized user. There is a risk your emails could be read or altered by unintended recipients. Although it is unlikely that someone will try to gain access to your

email, since email is sent over a wireless network, there’s a risk it may be intercepted. To decrease this risk, always choose to send emails over a secure wireless network.

If you have concerns about using an established email, you can establish a new email account (making sure to not include your name). It is easy to start a free webmail account [include link to suggested webmail signup, such as Gmail] completely for this purpose.²

Sample: Email - encryption
Email notifications are generally not secure, except in very limited circumstances, and should not be used to share or transmit research data. For this study, data will be encrypted when “in-transit,” or while being moved in the network to the secure storage location.